UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/626,420	07/24/2003	Sheueling Chang Shantz	6000-32301	9856

7590 03/02/2007

Robert C. Kowert
Meyertons, Hood, Kivlin,
Kowert & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/626,420	SHANTZ ET AL.	
	Examiner	Art Unit	
	Carlton V. Johnson	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-65* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-65* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7-4-2004/12-10-2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed on **7-24-2003**.

2. Claims **1 - 65** are pending. Claims **1, 18, 43, 50, 57, 61, 64, 65** are independent.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims **1 - 65** are rejected under 35 U.S.C. 101 because the claimed invention is based on non-statutory subject matter and directed towards nothing more than the abstract idea of a mathematical algorithm. Abstract ideas are not eligible for patent protection. A claimed invention reciting a computer program product that solely calculates a mathematical formula or a computer readable medium that solely stores a mathematical formula is not directed to the type of subject matter eligible for patent protection.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent

granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims **1 - 65** are rejected under 35 U.S.C. 102(e) as being anticipated by **Gressel et al.** (US Patent No. **6,748,410**).

Each independent section of the claimed invention will be addressed. The independent claim and the dependent claims based upon that independent claim recite instructions utilized to perform mathematical procedures or steps, such as multiplication and addition (i.e. summing), for an algorithm utilizing computer system processor(s) and system register(s).

Regarding Claims 1 - 17, Gressel discloses a method for operating a processor comprising: in response to executing a single arithmetic instruction, multiplying a first number by a second number; and adding implicitly a partial result from a previously executed single arithmetic instruction to generate a result that represents the first number multiplied by the second number summed with the partial result.
(see Gressel col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation; col. 2, lines 4-9; col. 5, lines 58-67: register usage; col. 8, lines 59-60: XOR operation; col. 2, lines 31-37: multiplication two values, sum two values utilizing partial (i.e. any bit length) result from previous multiplication)

Regarding Claims 18 - 42, Gressel discloses a method for operating a processor comprising: in response to executing a single arithmetic instruction, multiplying a first number by a second number; adding implicitly a partial result from a previously executed single arithmetic instruction; and adding a third number to generate a result that represents the first number multiplied by the second number summed with the partial result and the third number.
(see Gressel col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation; col. 2, lines 4-9; col. 5, lines 58-67: register usage; col. 8, lines 59-60: XOR operation; col. 2, lines 31-37: multiplication two values, sum two values utilizing partial (i.e. any bit length) result from previous multiplication)

Regarding Claims 43 - 49, Gressel discloses a processor comprising an arithmetic circuit, the processor responsive to execution of a single arithmetic instruction to cause the arithmetic circuit to multiply a first and second number and add implicitly a high order portion of a partial result from a previously executed single arithmetic instruction, thereby generating a result that represents the first number multiplied by the second number summed with the high order portion of the partial result.
(see Gressel col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate

cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation; col. 2, lines 4-9; col. 5, lines 58-67: register usage; col. 8, lines 59-60: XOR operation; col. 2, lines 31-37: multiplication two values, sum two values utilizing partial (i.e. any bit length) result from previous multiplication)

Regarding Claims 50 - 56, Gressel discloses a processor comprising an arithmetic circuit the processor responsive to a single arithmetic instruction that upon execution thereof causes the arithmetic circuit to multiply a first number and a second number and add a third number and implicitly add a high order portion of a previous result from a previously executed single arithmetic instruction thereby generating a result that represents the first number multiplied with the second number, summed with the high order portion of the previous result and with the third number.
(see Gressel col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation; col. 2, lines 4-9; col. 5, lines 58-67: register usage; col. 8, lines 59-60: XOR operation; col. 2, lines 31-37: multiplication two values, sum two values utilizing partial (i.e. any bit length) result from previous multiplication)

Regarding Claims 57 - 60, Gressel discloses a computer program product encoded on computer readable media, the computer program product comprising: a single arithmetic instruction causing a processor executing the single arithmetic instruction to

multiply a first number by a second number and implicitly add a high order portion of a previously executed single arithmetic instruction to generate a result that represents the first number multiplied with the second number and summed with a high order portion of a previously executed single arithmetic instruction, the single arithmetic instruction further causing the processor executing the single arithmetic instruction to keep a high order portion of the result for use with execution of a subsequent single arithmetic instruction.

(see Gressel col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation; col. 2, lines 4-9; col. 5, lines 58-67: register usage; col. 8, lines 59-60: XOR operation; col. 2, lines 31-37: multiplication two values, sum two values utilizing partial (i.e. any bit length) result from previous multiplication)

Regarding Claims 61 - 63, Gressel discloses a computer program product encoded on computer readable media, the computer program product comprising a single arithmetic instruction causing a processor executing the single arithmetic instruction to: multiply a first number by a second number; add implicitly a partial multiplication result from a previously executed single arithmetic instruction and a third number to generate a result that represents the first number multiplied by the second number summed with the partial multiplication result and summed with the third number; and store a high order portion of the result for use with execution of a subsequent single arithmetic instruction.

(see Gressel col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation; col. 2, lines 4-9; col. 5, lines 58-67: register usage; col. 8, lines 59-60: XOR operation; col. 2, lines 31-37: multiplication two values, sum two values utilizing partial (i.e. any bit length) result from previous multiplication)

Regarding Claim 64, Gressel discloses a processor comprising: means, responsive to a single multiply-accumulate instruction, for multiplying a first number with a second number and implicitly adding a partial result of a previously executed single multiply-accumulate instruction to generate a result that represents the first number multiplied by the second number summed with the partial result; and means for storing a high order portion of the result for use with execution of a subsequent single multiply-accumulate instruction.

(see Gressel col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation; col. 2, lines 4-9; col. 5, lines 58-67: register usage; col. 8, lines 59-60: XOR operation; col. 2, lines 31-37: multiplication two values, sum two values utilizing partial (i.e. any bit length) result from previous multiplication)

Regarding Claim 65, Gressel discloses a processor comprising: means, responsive to a single multiply-accumulate instruction, for multiplying a first number with a second number and implicitly adding a partial result of a previously executed single multiply-accumulate instruction, and for adding a third number to generate a result that represents the first number multiplied by the second number summed with the partial result and the third number; and means for storing a high order portion of the result for use with execution of a subsequent multiply-accumulate instruction.

(see Gressel col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation; col. 2, lines 4-9; col. 5, lines 58-67: register usage; col. 8, lines 59-60: XOR operation; col. 2, lines 31-37: multiplication two values, sum two values utilizing partial (i.e. any bit length) result from previous multiplication)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Carlton V. Johnson
Examiner
Art Unit 2136

C.J.

3/1/07

CVJ
February 26, 2007